ATTACHMENT 1

DRAFT

Review and Analysis of Privacy Related to the Bay Area Toll Authority FasTrak® Electronic Toll Payment Collection System

California State Senate Committee on Housing and Transportation
California State Assembly Committee on Transportation

December 1, 2010

Table of Contents

Executive Summary

In February 2010, the Bay Area Toll Authority (BATA) contracted with PricewaterhouseCoopers, LLP (PwC) to conduct a current state analysis of BATA's FasTrak® electronic toll collection system in regards to the privacy of customer data. This analysis was preparatory to the review required by California Assembly Bill 1175 (AB 1175) and to the associated mandatory report to Legislature due January 31, 2011. PwC is a nationally recognized independent entity with expertise in privacy issues associated with the electronic transmission and storage of data. The analysis emphasized the privacy and security of FasTrak® customer information as it is obtained, processed, and managed by BATA and related third parties, including the Regional Customer Service Center (RCSC) and Golden Gate Bridge, Highway and Transportation District (GGBHTD). The analysis considered the customer data elements collected as part of the FasTrak program and how they are processed, stored, destroyed and how they are secured throughout BATA's business activities.

Additionally, the results of the analysis included an independent perspective as to the maturity and sustainability of BATA's privacy and security capabilities. BATA, as a general practice, looks to leading practice as guidance – state agency privacy requirements, although not explicitly required, were considered as guidance to BATA in addressing observations identified in the analysis, along with leading industry practices, laws, regulations, statutes, and management frameworks.

In summary, based on the analysis conducted by PwC, it was found that:

1. The FasTrak® RCSC has the expected administrative and IT systems architecture controls in place to protect customer data and was deemed compliant in all areas of the Payment Card Industry (PCI) standards by a Qualified Security Assessor (QSA). Therefore, there is a low overall risk for data managed by the FasTrak® CSC.

2. BATA's internal policies and procedures in regards to privacy and security of customer data for the FasTrak® program should be strengthened.

In response to the findings and recommendations of the assessment, BATA is proposing updates to the FasTrak® Program Privacy Policy Customer Notice (BATA Resolution No. 96) to better explain to customers how their personal data is used, stored and protected and is developing and documenting internal policies and procedures to provide direction to agency staff regarding protecting customer data.

Due to the sensitive nature of the analysis workpapers and detailed outputs of the analysis, BATA has summarized the results into this report rather than release detailed information relating to the FasTrak infrastructure. This letter describes the activities conducted as required in

AB 1175 and subsequent activities to improve the privacy practices at BATA and in particular for the FasTrak® program.

Introduction / Background

Description of California Assembly Bill 1175 (AB 1175)

Legislative Mandate - AB1175 SEC. 9

"The Bay Area Toll Authority shall contract with a nationally recognized independent entity with expertise in privacy issues associated with the electronic transmission and storage of data to conduct a review and an analysis of the privacy issues associated with its electronic toll payment collection system. The report shall be transmitted to the Senate Committee on Housing and Transportation and the Assembly Committee on Transportation on or before January 31, 2011. The authority shall pay for the costs of the study from revenues available to the authority."

About the FasTrak® Program

Overview
The San Francisco Bay Area toll bridges consist of eight toll bridges. The seven state-owned bridges, Antioch, Benicia-Martinez, Carquinez, Richmond-San Rafael, Dumbarton, San Mateo Hayward and the San Francisco-Oakland Bay Bridge, are owned and operated by the California Department of Transportation (Caltrans). State toll bridge operations are funded by toll revenues, which are administered by the Metropolitan Transportation Commission, acting as the Bay Area Toll Authority. The Golden Gate Bridge is operated and funded by the Golden Gate Bridge, Highway and Transportation District (GGBHTD).

FasTrak® System
All eight toll bridges are equipped with Electronic Toll Collection (ETC), which has been dubbed "FasTrak" in California. All bridges have toll collection systems that include both manual and FasTrak capabilities. In addition, Bay Area customers are able to use their Title 21 based toll transponders on other California toll facilities with compatible ETC systems. This requires some level of data interchange to enable reciprocity of toll transactions between participating toll agencies. This interoperability does not require the exchange of customer personally identifiable information.

FasTrak allows customers to prepay bridge tolls, eliminating the need to stop at the toll plaza. The system has three components: a toll tag, which is placed inside your vehicle; an overhead antenna in the toll plaza, which reads the toll tag and automatically deducts the appropriate toll from your prepaid account; and video cameras to identify toll evaders. Processing of ETC toll transactions is conducted by BATA toll systems in conjunction with a third party processing center. The third party processor, referred to as the Regional Customer Service Center, handles the majority of customer personally identifiable information, including capturing customer profiles for enrollment and toll tag issuance, and customer service inquiries.

The FasTrak® program collects personal information from customers through FasTrak® enrollments and customer service interactions. Sensitive personal information collected includes

name, address, e-mail, credit card numbers, phone number, and vehicle information. Customer information is collected via the FasTrak website, phone calls, email, paper forms, fax, and in person. Once collected, customer information is inputted into the centrally managed RCSC data environment. BATA uses FasTrak® information to perform account reconciliations, oversee toll operations, and respond to escalated customer queries. BATA accesses FasTrak® information through private connections to the RCSC network. The RCSC interacts with FasTrak® customer information to process enrollments, toll collections, toll violations, customer service queries, and FasTrak® account changes.

All ETC transactions for all eight bridges are processed through the Regional Customer Service Center (RCSC). BATA maintains overall responsibility and accountability for the operation of the RCSC which is run by a private contractor under contract to BATA. BATA's contractual requirements are dictated in agreements with the third party that operates the center.

The RCSC maintains a comprehensive PCI compliant security program which includes processes and system configurations to enhance network, application, data, and physical security. See appendix for additional details regarding the RCSC's security program.

Privacy Analysis

Overview of 2010 FasTrak® Privacy Review and Analysis

The American Institute of Certified Public Accountants (AICPA) defines privacy as "Rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information". Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Objectives

The objectives of the FasTrak® analysis performed in 2010 were to evaluate privacy practices and security policies, procedures, technology and architecture as implemented by BATA to handle and protect sensitive FasTrak® customer information; to understand gaps in privacy and security capabilities, as compared to industry leading practices and specific state and federal regulations; to prioritize risks and construct a comprehensive plan to remediate key observations (see remediation actions below).

BATA engaged PwC to assist management with its FasTrak® Privacy Review and Analysis. PwC performed its assessment in accordance with the Standards for Consulting Services established by the American Institute of Certified Public Accountants and solely for the use and benefit of BATA management. They were not engaged to and did not conduct an examination, the objective of which would have been the expression of an opinion on compliance with specific privacy standards. Accordingly, PwC did not express such an opinion or audit or verify any information provided to them. Had PwC performed additional procedures, other matters might have come to their attention that would have been reported to BATA management.

Analysis Methodology

Analysis Framework

The Privacy Review and Analysis considered numerous laws, regulations, statutes, and leading practice frameworks and selected the Generally Accepted Privacy Principles (GAPP) framework. The analysis was performed using the GAPP framework as a benchmark for industry leading practices. These principles were formed by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). The analysis evaluated the maturity of the FasTrak® program based on the following criteria for privacy and security: Management, Notice, Choice and Consent, Collection, Use and Retention, Access, Disclosure to Third Parties, Security for Privacy, Quality, Monitoring and Enforcement.

Additionally, requirements in the Payment Card Industry (PCI) Data Security Standard (DSS) v1.2 framework were consulted as appropriate to supplement the analysis with regards to the credit card data handled by MTC/BATA, and with regards to evaluating the RCSC.

Architecture Review / Sensitive Data Flow Mapping

BATA, RCSC and other third party representatives were interviewed to understand the privacy and security architecture of the FasTrak® program. Departments interviewed included finance, legal, IT, operations, public information, general management, etc. The interviews were conducted to understand the roles and responsibilities of the involved agencies and third parties, their interdependencies, contractual obligations, shared technologies, etc. The results of the architecture review were reviewed with management to appropriately scope assessment test plans. Additionally, a sensitive data flow diagram was created, capturing the transmission, storage and treatment (i.e. encryption) of sensitive data.

Policies, Procedures and Other Documentation Review

BATA and the RCSC provided several privacy and security policies and procedures for review during the analysis. These included: information security and privacy policies such as retention, disposal, acceptable use, education, training, and confidentiality agreements; description of roles and responsibilities; business process narratives or other documentation describing agency processes related to FasTrak® and backend processes using customer information; FasTrak® agreements and contracts; prior privacy and security related assessments; asset inventories or data flow descriptions for systems storing and processing customer PII; system security procedures and configuration standards; and other relevant documents.

Security Configuration Reviews

A FasTrak® sensitive data flow map was created to identify systems processing, storing, or transmitting sensitive customer information. A representative sample of BATA and RCSC systems were selected for configuration review. The security analysis relied on prior assessment

results for systems that were recently assessed via internal controls, PCI or other assessments. The majority of security testing was performed on the BATA systems.

RCSC management validated that their PCI policies, procedures, controls and architecture are used to manage and protect all sensitive customer information, and not just credit cards. Therefore, the analysis relied heavily on the RCSC's annual PCI certification for assurance which was not part of the scope of the Privacy Review and Analysis.

Interviews and Validation

Analysis observations were confirmed with BATA, RCSC and other third parties' personnel via interviews and emails. Additionally, a privacy workshop was held with agencies involved (excluding the third party RCSC) to discuss scope and implications of the findings.

Analysis Results and Remediation Actions

Per the analysis, it was noted that the majority of FasTrak customer information is processed and stored by the third party operator of the FasTrak® RCSC, which is contracted by BATA. This third party contractor was deemed compliant in all areas of PCI-DSSv1.2 by a Qualified Security Assessor. Additionally, FasTrak customer information, beyond credit cards, is also protected by the RCSC's PCI policies, procedures, controls and security architecture.

Additionally, per the analysis of privacy and security processes and procedures implemented by BATA, it was concluded that BATA did not initially meet all compliance requirements and industry best practices associated with privacy and security. Since the analysis was concluded, BATA has undertaken a process to formalize its privacy and security program, as well as address specific areas of improvement identified by the independent third party reviewer's analysis.

Summary of Observations

BATA does not sell the customer's personally identifiable information (PII), and notifies users how their data is generally used and protected. High value is placed on addressing customer concerns and complaints. Additionally, the majority of data privacy and security functions are outsourced to the third party RCSC, which significantly reduces the risk by limiting BATA's storage and processing of PII.

The following opportunities for improvement for BATA resulted from the analysis: formalize governance structure for privacy, security and compliance monitoring; create internal policies, procedures and standards for privacy, security, confidentiality, training, incident response, data classification, and data retention; standardize third party contracts to address information security and privacy (certain contracts do have these provisions); sufficiently segment FasTrak® data since use of corporate services from MTC (e.g., email and file shares) result in PII residing outside BATA's network and controls; increase security protections for PII stored in BATA and MTC environments, as security testing revealed vulnerabilities that could be exploited to expose

FasTrak® data; expand understanding of regulatory landscape that is relevant to BATA and MTC.

Following the analysis in June 2010, BATA is strengthening its controls around privacy policies, processes, and technology. In summary, the following enhancements were made to the privacy program to remediate gaps identified in the analysis:

- Assignment of privacy governance roles and responsibilities
- Development of formal internal privacy policies and procedures for BATA's employees
- Reviewing and strengthening of information technology security policies and system configurations
- Strategic planning for additional technology and infrastructure solutions in the long term
- Clarifications and revisions to the privacy notice posted on the FasTrak® web site
- Development of privacy training for appropriate BATA employees

Observations and Remediation Actions

Management

Observations

Privacy stakeholders, roles and responsibilities are not formally defined and there is no single group accountable for privacy. Additionally, there is no cross-functional team across departments (Legal, HR, Finance, Operations, IT, etc) and across agencies (BATA, GGBHTD, RCSC, etc) to coordinate the privacy program. Several departments are working in silos to address similar issues, resulting in duplicative and conflicting efforts.

Formalized privacy policies do not exist, such as data classification, data transmission via email, data retention, etc. Additionally, security policies are not fully implemented. There is no clear responsibility for centrally managing, updating and communicating the policies, including training and education. Security policies are not based on industry standard frameworks and do not reference each other. Formal security incident response and related process flows for privacy breach scenarios do not exist and a formal ownership of the incident response process does not exist.

Remediation Actions

BATA is developing a Privacy Policy Executive Director Management Memorandum (Privacy Policy EDMM), to direct the efforts of BATA staff in regards to protecting customer data. The Privacy Policy EDMM:

- Provides policy and procedural direction to BATA employees in regards to protecting customer data. The Privacy Policy EDMM defines and classifies personally identifiable information (PII) and dictates guidelines on how such information should be used and handled.
- Establishes a governance structure to oversee privacy within the organization, which includes designating a Privacy Officer within the Office of General Counsel.

- Provides an incident response checklist with defined roles and responsibilities to be used in the event of a data breach or security incident to ensure relevant actions are performed in a timely manner.
- Requires in-person privacy training sessions for employees, to inform employees of roles, responsibilities, and guidelines detailed in the privacy and security policies. Training for employees included interactive privacy questions and walkthroughs of relevant data handling scenarios
- Establishes the development of information technology security policies to include guidance around security requirements and access restriction.

Notice

Observations
There is no process to periodically review and update the web site and the forms used to collect personal information (online and paper). Associated privacy statements are not regularly reviewed to ensure that they accurately reflect current practices. Additionally, some forms that collect personal information do not contain privacy statements.

Remediation Actions
The Privacy Policy EDMM assigns responsibility for maintaining and updating privacy notices to the Privacy Officer.

Choice and Consent

Observations
Although stated elsewhere on the website, opt-out procedures, privacy contact information, and the RCSC's role in account processing are not explicitly stated in the privacy notice.

Remediation Actions
The FasTrak® Program Privacy Policy Customer Notice displayed on the FasTrak® website is being revised to provide customers more transparency into how data is collected, used, and processed. The notice is being revised to specifically include information about the RCSC's role in account processing and customer contact information at BATA and the RSCS in regards to privacy matters.

Collection

Observations
The FasTrak website stores cookies, but the web privacy statement does not address the use of cookies.

Remediation Actions
The FasTrak® Program Privacy Policy Customer Notice is being revised to provide details about web cookies collected on the FasTrak® website to provide customers more insight into information collected.

Use and Retention

Observations

Privacy policies do not address record retention for FasTrak® PII, and there is a lack of formal use and retention procedures or knowledge for FasTrak® PII. Additionally, the record retention policy used by the RCSC, as determined by their contract with BATA, states that closed account information is retained through the contract duration; however, under SB1268, as of July 1, 2011, closed account information must be purged after 4 years and 6 month.

Remediation Actions

The FasTrak® Program Privacy Policy Customer Notice and the Privacy Policy EDMM are being updated to state the data retention guidelines for customer PII. BATA will limit the retention of customer information collected and purge all PII for closed accounts within four years and six months after the date an account is closed or terminated. Additionally, to increase knowledge in regards to record retention at BATA and other policies relating to privacy and security, BATA has begun delivering privacy training sessions to appropriate BATA employees.

Access

Observations

The process of providing FasTrak customers access to their personal information is currently ad-hoc, however BATA is capable of responding to these requests.

Remediation Actions

The FasTrak® Program Privacy Policy Customer Notice was revised to clearly inform customers how to update their personal information maintained by the FasTrak® program. The notice includes contact information at the FasTrak® RCSC and at BATA to revise data or to make inquiries about customer data. Additionally, the Privacy Policy EDMM directs that the BATA Privacy Officer is responsible for responding to requests from customers in regards to their PII.

Disclosure to Third Parties

Observations

BATA contracts contain general confidentiality clauses stating that customer data should only be used for the stated purposes and that the contracted entities abide by all laws and regulations. However, contracts do not specifically address the following in a standardized manner: formal privacy and security policies; defined security and privacy requirements for employees; non-disclosure agreement; record retention policy; data breach notification/incident response; subcontracting; and right to conduct privacy assessments.

Remediation Actions

The Privacy Policy EDMM includes specific language to be included in third party contracts to assist in ensuring that third party contractors protect customer data.

Security for Privacy

Observations
MTC and BATA's security policies are not fully defined or implemented. Several technologies are out of date. Alerting systems such as IDS/IPS are missing and security event monitoring and formal log review processes are not in place. Management is informed of security issues on an ad-hoc basis. Additionally, there is no formal/standardized encryption solution in use, such as PGP.

Remediation Actions
BATA is currently updating the information technology security policy and will define security roles and responsibilities to enhance security for privacy. BATA is also updating system configurations based on findings from the privacy analysis. All security findings from the privacy analysis are prioritized, tracked, and assigned to owners for action. Remediation tasks which require more substantial investment in technology and infrastructure are being reviewed.

Monitoring and Enforcement

Observations
A privacy compliance function does not exist for FasTrak®, and compliance activities are not centralized as several different groups own different aspects of compliance. Consequently, privacy compliance is not monitored and tracked. Existing business practices are not evaluated to ensure compliance with Privacy and Security requirements. Additionally, handling and use of sensitive FasTrak® data by internal or third party resources is not monitored or enforced.

Remediation Actions
The Privacy Policy EDMM establishes processes for monitoring privacy and security issues, including defining roles and responsibilities for BATA staff to monitor FasTrak privacy and security activities and track and enforce compliance to key regulations and standards.

GOOD FAITH RESPONSE TO LEGISLATION

BATA, its partners, and affiliates coordinate jointly to maintain the privacy of customer information. BATA has responded to this legislative requirement by conducting the required analysis, has implemented short term improvements identified, and has planned longer term solutions to maintain a privacy program that meets both legislative and customer expectations.

COMMENT ON SB1268

BATA's privacy program is committed to privacy improvement and maintaining compliance with changing privacy laws and regulations. BATA is considering California Senate Bill 1268 as it defines appropriate mechanisms to protect and prevent misuse of customer information. This bill limits electronic toll transportation agencies in their use of personal information collected from subscribers to toll systems. Toll Transportation agencies are prohibited from selling customer information. Transportation agencies are required to establish a privacy policy

regarding use of personally identifiable information. In particular, transportation agencies are not allowed to sell personal information. The bill also sets requirements on data retention, stating in no case shall a transportation agency retain any information on closed accounts more than 4.5 years after an account is terminated.

Appendix

FasTrak® Program Privacy Policy Customer Notice